1. FIN scans: like ghost-knocking on digital doors!

A `FIN scan` is a network reconnaissance technique used to identify open ports on a target machine. It works by sending a `TCP` packet with only the `FIN` flag set, which typically signifies the end of a connection. By analyzing the target's response, attackers can determine if a port is open, closed, or filtered by a firewall.

`FIN` scans are attractive because they can sometimes bypass basic firewalls and offer a stealthier approach compared to traditional methods.

Write a bash script that executes a `FIN scan` on a test network.The scan should identify potential stealth ports, focusing on ports `80` to `85`.

- Your script should accept `host` as an arguments `$1`.
- Your script should use packet fragmentation to evade packet filters.
- Your script should Adjust the timing option to `2` to reduce scan detectability.

Depending on the scanned network, the output could change, this scan may require some time to finish.

```
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─🏴 ./1-fin_scan.sh www.holbertonschool.com
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-22 13:30 CET
Nmap scan report for www.holbertonschool.com (52.17.119.105)
Host is up (0.17s latency).
Other addresses for www.holbertonschool.com (not scanned): 63.35.51.142 34.249.200.254 64:ff9b::3411:7769 64:ff9b::22f9:c8fe 64:ff9b::3f23:338e
rDNS record for 52.17.119.105: ec2-52-17-119-105.eu-west-1.compute.amazonaws.com

PORT   STATE         SERVICE
80/tcp open|filtered http
81/tcp open|filtered hosts2-ns
82/tcp open|filtered xfer
83/tcp open|filtered mit-ml-dev
84/tcp open|filtered ctf
85/tcp open|filtered mit-ml-dev

Nmap done: 1 IP address (1 host up) scanned in 17.14 seconds
```

```
sudo nmap -sF -f -T2 $1
```